

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of)	
1996)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer)	
Proprietary Network Information and Other)	
Customer Information)	
)	
Petition for Rulemaking to Enhance Security and)	
Authentication Standards for Access to Customer)	RM-11277
Proprietary Network Information)	
<hr/>)	

**JOINT REPLY COMMENTS OF ESCHELON TELECOM, INC., SNIP LINK INC., AND
XO COMMUNICATIONS, INC.**

John J. Heitmann
Jennifer M. Kashatus
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8400 (telephone)
(202) 342-8451 (facsimile)

June 2, 2006

SUMMARY

The comments submitted in this proceeding demonstrate that the security breach of which EPIC complained in its Petition is substantially more limited than either EPIC or the Commission had speculated. Record evidence demonstrates that any security breaches that might have occurred are the result of unscrupulous data brokers, and are not due to lack of security protections by telecommunications carriers.

The lack of a widespread problem and the presence of carrier-specific privacy measures further emphasizes that there simply is no need to modify the Commission's existing CPNI rules. The record is replete with evidence from carriers in all industry segments, including competitive local exchange carriers ("CLECs"), incumbent local exchange carriers ("ILECs"), and wireless carriers, that EPIC's proposals are unduly burdensome and extremely costly to implement, while at the same time not solving the underlying problem—the actions of the data brokers. Therefore, the Commission should decline to adopt any of EPIC's proposals including the implementation of: (1) consumer-set passwords; (2) audit trails; (3) encryption; (4) data retention; and (5) notice requirements. Instead, the Commission should work with the Federal Trade Commission on enforcing existing rules to curb and deter the practices of unlawful data brokers.

The Joint Commenters support the implementation, in theory, of safe harbor protection for carriers. Although neither party proposing a safe harbor (AT&T and Verizon) provided specifics about their proposed safe harbor, the Joint Commenters generally support a safe harbor that would prevent carriers from being liable if it has adopted appropriate safeguards in accordance with the Commission's CPNI rules.

The Joint Commenters also support COMPTTEL's request that the Commission prevent ILECs from mandating that CLECs relinquish control over their own customers' CPNI. As COMPTTEL demonstrated in its comments, under AT&T's commercial agreements, AT&T reserves the right to provide CPNI of the CLEC's customers to third parties. The commercial agreements also require CLECs to indemnify ILECs for any improper disclosure of the CLEC's customer CPNI. The Joint Commenters support COMPTTEL's request that the Commission make clear that the language included in AT&T's commercial agreements and any other language that hampers a carrier's ability to protect the CPNI of its own customers will be deemed unenforceable.

Lastly, the Commission should not apply its current CPNI rules or any rules adopted as a result of this proceeding to Internet Service Providers or to non-telecommunications services (such as information services) provided by telecommunications providers. Section 222 of the Act solely extends to "telecommunications services" and does not apply to records associated with information services.

As is evident from the comments, carriers have demonstrated a commitment to customer privacy. Carriers should be permitted to devise their own privacy protections that work for their particular situation and should not be forced into a one-size fits all mold. Therefore, the Joint Commenters request that the Commission refrain from modifying its CPNI rules in any form, and instead focus on enforcing the current rules.

TABLE OF CONTENTS

	Page
I. THE COMMENTS DEMONSTRATE THAT THE COMMISSION SHOULD REJECT EACH OF EPIC'S PROPOSALS	3
A. Consumer-Set Passwords.....	3
B. Audit Trails	5
C. Encryption.....	7
D. Data Retention	7
E. Notice Requirements.....	8
F. Other Protections	9
II. THE JOINT COMMENTERS SUPPORT THE IMPLEMENTATION OF A SAFE HARBOR	9
III. THE JOINT COMMENTERS SUPPORT COMPTEL'S REQUEST THAT THE COMMISSION PREVENT ILECS FROM MANDATING CLECS TO RELINQUISH CONTROL OVER THEIR CUSTOMERS' CPNI	12
IV. THE COMMISSION SHOULD NOT APPLY ITS CURRENT CPNI RULES OR ANY RULES ADOPTED AS A RESULT OF THIS PROCEEDING TO INTERNET SERVICE PROVIDERS OR INFORMATION SERVICES.....	13
V. CONCLUSION.....	14

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Implementation of the Telecommunications Act of 1996)	CC Docket No. 96-115
)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information)	
)	
Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information)	RM-11277
)	
_____)	

**JOINT REPLY COMMENTS OF ESCHELON TELECOM, INC., SNIP LINK INC., AND
XO COMMUNICATIONS, INC.**

Eschelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc.

(collectively, "Joint Commenters"), through their attorneys and in accordance with the public notice adopted in this proceeding,¹ respectively submit their reply comments in the above-captioned proceeding. Evidence in this record demonstrates that the scope of the problem that EPIC has identified through its Petition is substantially more limited than either EPIC or the Commission had speculated. Like the Joint Commenters, many of the commenters in this proceeding state that, to the best of their knowledge, they have not experienced any security

¹ See *Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115; *Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*; *Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, RM-11277, Notice of Proposed Rulemaking, FCC 06-10 (rel. Feb. 14, 2006); *Wireline Competition Bureau Grants Request for Extension of Time to File Reply Comments in Response to the Commission's Notice of Proposed Rulemaking to Enhance Security and Authentication Standards for Access to CPNI*, Public Notice, CC Docket No. 96-115, DA 06-1033 (May 15, 2006).

breaches that have resulted in an unlawful disclosure of CPNI.² Additionally, all carriers in this proceeding have demonstrated a commitment to customer privacy, and have taken varying measures designed for their particular size and circumstances to protect customer privacy.

The lack of a widespread problem and the presence of carrier-specific privacy measures further emphasizes that there simply is no need to modify the Commission's existing CPNI rules. The record is replete with evidence from all carriers, whether incumbent local exchange carriers ("ILECs"), competitive local exchange carriers ("CLECs"), and wireless carriers that the safeguards EPIC has proposed are unduly burdensome and extremely costly to implement. In addition to the burdens and costs, these proposals are problematic because they are misdirected at carriers instead of the root of the problem: the unscrupulous data brokers. Therefore, the Commission must reject each of EPIC's proposals. Instead, the Commission should focus its efforts on working with the Federal Trade Commission ("FTC") to enforce existing rules and combat unlawful practices by data brokers.

In these reply comments, the Joint Commenters will not reiterate all of the arguments set forth in their initial comments. Instead, the Joint Commenters will respond to the following specific issues: (1) the Commission must reject each of EPIC's proposals as the costs and burdens associated with those proposals far outweigh any possible benefit; (2) the Joint Commenters support the implementation of a safe harbor; (3) the Joint Commenters support COMPTTEL's argument that the Commission must emphasize that CLECs cannot be forced to accept language in their commercial agreements that requires them to relinquish control over CPNI or to indemnify ILECs for the misuse of their customers' CPNI; and (4) the Joint

² See, e.g., Comments of Leap Wireless International at 4; Comments of MetroPCS Communications at 2; Comments of Texas Statewide Telephone Cooperative at 3.

Commenters oppose extending the CPNI rules to Internet Service Providers (“ISPs”) or to information services provided by telecommunication carriers.

I. THE COMMENTS DEMONSTRATE THAT THE COMMISSION SHOULD REJECT EACH OF EPIC’S PROPOSALS

The comments in this proceeding from all industry segments unequivocally demonstrate that the Commission should reject each of EPIC’s proposed safeguards, because, contrary to the proponents’ arguments, they are extremely costly, unduly burdensome, and are not directed toward the bad actors: the data brokers. Regardless of the industry segment, all carriers (wireless and wireline) and cable operators uniformly demonstrate that protecting consumer privacy is of the utmost importance to their operations.³ Therefore, carriers already have implemented security procedures that are appropriate for their particular company; carriers should not now be forced to implement a one-size-fits all approach that, as a practical matter, will have little (if any) appreciable benefits on protecting consumer privacy.

A. Consumer-Set Passwords

The Commission must reject the few comments arguing that carriers should be required to implement consumer-set passwords.⁴ As an initial matter, the record is replete with evidence that consumers do not want to secure their records with a consumer-set password.⁵

³ See, e.g., Comments of T-Mobile USA at 4; Comments of Time Warner at 5; Comments of Verizon at 1.

⁴ See, e.g., Comments of Princeton University Students at 9 (arguing that “passwords can be an effective deterrent against unauthorized access to a user’s phone records.”).

⁵ See, e.g., Comments of Centennial Communications Corp. at 4 (stating that 63% of respondents of a recent poll stated that it is inconvenient to remember passwords); AT&T Comments at 8 (stating that 87% of customers are opposed to the use of passwords); Comments of Qwest Communications International Inc. at 20-22 (stating that forcing customers to use passwords will lead to customer discontent). The Joint Commenters also incorporate their initial comments outlining the costs and burdens that they would

Comments in this proceeding overwhelmingly demonstrate that the implementation of consumer-set passwords would come at great costs and burdens to carriers without the receipt of any appreciable security improvement in return.⁶ To implement a consumer-set password scheme, many carriers would need to develop new databases and systems equipped to handle the passwords.⁷ These systems could cost hundreds of thousands of dollars simply to implement.⁸ After implementation, carriers then would need to use resources to monitor and update the databases as well as to respond to consumer inquiries regarding lost and forgotten passwords. Consumer-set passwords are particularly problematic for business customers, where frequently more than one person is an authorized representative, and the loss of the password would require resetting the password for the entire company.⁹

The great costs and burdens associated with implementing consumer passwords would come without any appreciable consumer security benefit.¹⁰ The record in this proceeding demonstrates that the greatest security breach appears to be pretexting.¹¹ Yet, even certain commenters supporting additional security protections recognize that consumer-set passwords

incur as a result of the implementation of consumer-set passwords. *See* Comments of Joint Commenters at 5-7.

⁶ *See, e.g.*, AT&T Comments at 10; Comments of Time Warner Telecom at 12; BellSouth Comments at 16-17.

⁷ *See* Comments of Texas Statewide Telephone Cooperative at 4.

⁸ Comments of Verizon at n. 14.

⁹ *See, e.g.*, Comments of Time Warner Telecom at 12 (stating that consumer-set passwords, particularly in the form of a “shared secret,” are troublesome for business customers, because if one person in the company forgets the password, then the entire company password system must be reset).

¹⁰ *See* Comments of the Joint Commenters at 5-7.

¹¹ *See* Comments of COMPTTEL at 3; Comments of Verizon at 3.

are inadequate to prevent the types of security breaches that are occurring.¹² As several comments in this proceeding demonstrate, consumer-set passwords are an inefficient means to secure customer data, because pretexters easily can bypass password protection.¹³ If a data broker is able to obtain personal information about the customer, then it likely can obtain the necessary password to access the account or sufficient information to request that the password be reset such that it can access the account. Therefore, the costs and burdens associated with implementing consumer-set passwords, the lack of consumer interest in such passwords, and the minimal security protections that consumer-set passwords will bring demonstrates that the Commission should reject EPIC's proposal to implement consumer-set passwords.

B. Audit Trails

The vast majority of comments in this proceeding demonstrate that the burdens of implementing an audit trail substantially outweigh any potential benefit. The Joint Commenters therefore strongly oppose the few comments (AT&T, NASUCA, the New Jersey Ratepayer Advocate, and Princeton University Students) that support the implementation of an audit trail and that suggest that implementing an audit trail would be a simple process.¹⁴ In 1999, the

¹² See Comments of the National Association of State Utility Consumer Advocates at 15-17 (hereinafter "NASUCA Comments"); *but cf.* Comments of Princeton University Students at 9 (arguing that consumer-set passwords would be effective against pretexting).

¹³ See, e.g., Comments of Time Warner Telecom at 12 (stating that passwords are ineffective because pretexters easily can have a password reset); US LEC Comments at 2-4 (stating that there is no guarantee that CPNI is safe even with consumer-set passwords).

¹⁴ See, e.g., NASUCA Comments at 10-11 (stating that many carriers already have tracking systems in place); Comments of the New Jersey Ratepayer Advocate at 4 (stating that the "marginal cost to also record disclosure to purported account holders should be small."); Comments of Princeton University Students at 4 (stating, "[f]or large companies, making records of access to sensitive data should be minimally costly, since these companies already make audits for certain types of access..."). Even Princeton acknowledges, however, that smaller companies "may find it more difficult to create auditing systems," but it has failed to define what it classifies as a small or large company, leaving the comments open to interpretation and erroneous assumptions. See also Comments of Joint Commenters at 7 (outlining their objections to the implementation of an audit trail).

Commission rejected its proposal to implement an audit trail on the ground that it would be too costly for carriers to implement.¹⁵ In doing so, the Commission recognized that there would be “‘massive’ data storage requirements at great cost” to carriers.¹⁶

The costs that led to the Commission’s rejection of this burdensome requirement in 1999 remain equally applicable today, thus necessitating that the Commission reject EPIC’s proposed detailed audit trail requirement. As the Joint Commenters already have explained, and additional comments in this proceeding support, it would be extremely costly and burdensome for carriers to change or modify their databases to create the specific type of audit trail that the Commission proposes in the *NPRM*.¹⁷ In addition, as Qwest demonstrated in this proceeding, the adoption of audit trails would lead to increased costs for data storage, extensive updates to existing application software and the collection of information to be stored for later auditing.¹⁸ Similarly, US LEC argued that, like the Joint Commenters, it would be required to change its system at a substantial cost to be able to accommodate the type of audit trail that the Commission has proposed.¹⁹

¹⁵ See *Implementation of the Telecommunications Act of 1996; Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, 14 FCC Rcd 14409 (1999) (“*CPNI Reconsideration Order*”); see, e.g., Comments of Qwest Communications International Inc. at 13 (citing to the *CPNI Reconsideration* and noting that the costs today still would be great); Comments of Verizon Wireless at 12-14 (arguing that there is no reason for the Commission to reverse its prior decision rejecting the use of an audit trail).

¹⁶ *CPNI Reconsideration Order* at 14474-75, ¶ 127 (citations omitted).

¹⁷ See Comments of the Joint Commenters at 7; see also Comments of Qwest Communications International Inc. at 15 (stating that data storage costs associated with the type of audit trail that EPIC proposes would cause massive data storage requirements along with costs for “extensive updates to existing application software.”).

¹⁸ Comments of Qwest Communications International at 15.

¹⁹ Comments of US LEC Corp. at 4.

Although these audit trails would come at a great cost to the carriers, there would be no beneficial result. Indeed, even AT&T, a supporter of audit trails, acknowledges that “audit trails may be of limited utility....”²⁰ As Verizon Wireless explains, “there is no nexus between requiring audit trails and stopping pretexting, because no amount of recordkeeping after the fact will prevent a pretexter from obtaining CPNI.”²¹ Accordingly, the Commission once again should reject the proposal to implement an audit trail, finding that the costs associated with implementing an audit trail far outweigh any potential benefits as a result thereof.

C. Encryption

The comments in this proceeding also overwhelmingly demonstrate that the burdens associated with implementing an encryption system far outweigh any potential benefit of encrypting CPNI.²² Although certain commenters, such as the New Jersey Ratepayer Advocate argue that encryption “would be helpful,”²³ as a practical matter, encryption would not derive the benefits that EPIC has promised. Specifically, encrypting the data will do little to deter a pretexter’s ability to access the data.²⁴ Since the vast majority of security breaches appear to occur through pretexting, encrypting data will not respond to this particular security concern and the costs and burdens of encrypting data cannot be justified.²⁵

D. Data Retention

The Joint Commenters agree with the comments in this proceeding that overwhelmingly demonstrate the substantial hardship that would occur as a result of limiting

²⁰ AT&T Comments at 14.

²¹ Comments of Verizon Wireless at 13.

²² AT&T Comments at 15-16; Comments of Joint Commenters at 8.

²³ Comments of the New Jersey Ratepayer Advocate at 4.

²⁴ AT&T Comments at 15-16.

²⁵ Comments of Joint Commenters at 8; *see also* Comments of AT&T at 16.

data retention and implementing mandatory document destruction procedures.²⁶ Indeed, even the federal government opposes implementing data retention. Specifically, the United States Departments of Justice and Homeland Security demonstrate that mandatory document destruction would hamper their investigations.²⁷ Additionally, the Joint Commenters agree with those commenters that argue that mandatory document destruction would be detrimental to a carrier's ability to preserve its rights in the event of a carrier dispute, such as a billing dispute.²⁸ The Commission, therefore, should reject EPIC's proposal to implement mandatory data destruction.

E. Notice Requirements

The Joint Commenters also agree with those commenters that argue that the Commission should decline to impose notice requirements proposed by EPIC.²⁹ As proposed, the Commission would require carriers to notify customers of a *potential* security breach as well as every time that the carrier released the customer's CPNI. The Joint Commenters agree with Verizon Wireless that doing so "would cause unnecessary distress and confusion for customers because the carrier would not necessarily know of the breach."³⁰ Furthermore, as Verizon Wireless explains, the Commission's proposal establishes an "impossible compliance obligation" since the carrier would not have sufficient information to determine whether its notification obligation had been triggered in the first instance.³¹ Therefore, the Commission should not adopt

²⁶ See, e.g., Comments of the United States Departments of Justice and Homeland Security at 4-7; Comments of Joint Commenters at 8-9.

²⁷ Comments of the United States Departments of Justice and Homeland Security at 4-7.

²⁸ See, e.g., Comments of US LEC Corp. at 5 (stating, "a Commission-imposed time period that limits a carrier's ability to retain records may conflict with other requirements under federal laws and regulations.").

²⁹ Comments of Verizon Wireless at 15-16; see Comments of Joint Commenters at 9-11.

³⁰ See Comments of Verizon Wireless at 15.

³¹ See *id.* at 16.

the proposed notice requirements, which are unnecessarily burdensome without any corresponding benefit.

F. Other Protections

The Joint Commenters do not oppose the Commission's proposed rule change, as supported by several carriers in this proceeding, to require carriers to file their annual CPNI certification with the Commission.³² The Joint Commenters, however, agree with the comments in this proceeding stating that if the Commission imposes such a regulation, then the Commission should require parties to file their CPNI certification by a date certain for administrative convenience.³³

II. THE JOINT COMMENTERS SUPPORT THE IMPLEMENTATION OF A SAFE HARBOR

The Joint Commenters support Verizon's and AT&T's proposals to establish a "safe harbor" protection for carriers.³⁴ Neither carrier has fleshed out the details of the proposed safe harbor, but in theory, a carrier would not be liable for the unlawful penetration of its system (for example, through pretexting) if it has adopted appropriate safeguards in accordance with the Commission's CPNI rules.³⁵ The Joint Commenters agree that establishing the type of reasonable practices that will be developed to receive the "safe harbor" protections will allow carriers the necessary flexibility they need to protect their customers' information from data brokers that will continue to find ways to circumvent safeguards implemented by carriers to

³² See AT&T Comments at 6, 14-15.

³³ See *id.* at 15.

³⁴ See Comments of Verizon at 2.

³⁵ *Id.*

obtain CPNI.³⁶ As discussed herein, however, absent additional information about the safe harbor, the Joint Commenters cannot agree at this time with each of the safe harbor components that Verizon has identified. The Joint Commenters also submit that any safe harbor that the Commission adopts must grant carriers immediate protection once the carrier is required to disclose CPNI to any person or entity and for any purpose.

Although the Joint Commenters agree with the concept of a safe harbor, in the absence of additional information about the interworking of Verizon's proposal,³⁷ the Joint Commenters are unable to support each prong of the safe harbor that Verizon has enumerated. Based on the information specified in Verizon's comments, the Joint Commenters generally support each of the following safe harbor components that Verizon has proposed as they are reasonable practices for protecting customer privacy: (1) cooperating with FCC, FTC and DOJ efforts to identify and prosecute data brokers; (2) participating in a carrier working group dedicated to enhancing data security and combating theft of confidential information; (3) posting privacy policies online; and (4) establishing certain categories of information that should not be disclosed to customers.³⁸

Without additional details about the safe harbor proposal, however, at this time, the Joint Commenters are unable to support the remaining two components of the safe harbor: (1) filing detailed CPNI certifications with the Commission; and (2) implement voluntary password protection. Consistent with the above comments, the Joint Commenters do not oppose the proposed rule change that all carriers must file their annual CPNI certification with the

³⁶ *Id.* at 2-3.

³⁷ AT&T does not identify specific safe harbor criteria.

³⁸ *See* Comments of Verizon at 11-12.

Commission.³⁹ In the annual certification, carriers already are required to provide information about their security efforts. The Joint Commenters are unclear what additional information Verizon would propose to include in the safe harbor, but cautions that filing too much information, even under seal, always invites a potential security risk.

Absent additional information, the Joint Commenters also cannot endorse a voluntary consumer-set password approach for residential customers as part of the safe harbor. As stated above, the Joint Commenters oppose the implementation of a mandatory consumer-set password requirement for all carriers, citing the high costs of implementing such a program and the limited benefit that would result therefrom.⁴⁰ Indeed, Verizon's own position regarding consumer-set passwords is unclear; it appears that Verizon supports the implementation of voluntary consumer-set passwords for residential customers as part of its safe harbor, yet recognizes that implementing consumer-set passwords would place a large burden on carriers that do not already have the mechanisms to implement such passwords.⁴¹ Specifically, Verizon argues that mandatory customer-set password program will come at a great expense to carriers,⁴² and may actually decrease the security of customer data.⁴³ Therefore, the Joint Commenters do not have sufficient information to address this aspect of the safe harbor proposal.

The Joint Commenters also submit that any "safe harbor" program that the Commission implements must grant immediate protection to carriers as soon as the carrier is

³⁹ See *supra* section I.F.

⁴⁰ See *supra* section I.A.

⁴¹ See Comments of Verizon at 4-8.

⁴² See Comments of Verizon at 5-7. Verizon provides evidence that more than 80 percent of people have forgotten their passwords; that between 10 to 30 percent of help desk calls are for requests to reset passwords; that it costs between \$100 to \$350 per user per year to manage passwords and between \$51 to \$147 in labor costs to reset passwords. See *id.*

⁴³ *Id.* at 8.

required to disclose the information for any purpose. As one example, the safe harbor must be triggered as soon as the carrier releases information to its billing agent, and, at a minimum, no later than when the consumer receives the bill. There are many legitimate business reasons that carriers must release CPNI. Once the carrier releases CPNI, even with the most ardent protections (including, for example, safeguards in contracts with all agents requiring the agent to safeguard the confidential information), the carrier no longer has control of the CPNI. The carrier cannot guarantee that third parties, including customers themselves, will protect their own data. Any safe harbor protection, therefore, must extend protection from liability at the time a carrier is required to disclose the customer information for any reason.

III. THE JOINT COMMENTERS SUPPORT COMPTTEL'S REQUEST THAT THE COMMISSION PREVENT ILECS FROM MANDATING CLECS TO RELINQUISH CONTROL OVER THEIR CUSTOMERS' CPNI

The Joint Commenters support COMPTTEL's request that the Commission affirmatively oppose language in commercial agreements that would require CLECs to relinquish their control over their customers' CPNI. In its comments, COMPTTEL explained that in SBC's (now AT&T's) Local Wholesale Complete commercial agreement, AT&T reserves the right to access the CPNI of the CLEC's customers without the CLEC's knowledge. Under the agreement, AT&T also reserves the right to provide CPNI of the CLEC's customers to third parties.⁴⁴ The commercial agreements also require CLECs to indemnify ILECs for any improper disclosure of the CLEC's customer CPNI.⁴⁵ According to COMPTTEL, each of these provisions is non-negotiable. The Joint Commenters agree with COMPTTEL that AT&T's CPNI practices described in the commercial agreements directly contravene the Commission's policy to

⁴⁴ See Comments of COMPTTEL at Exhibit 1.

⁴⁵ See *id.* at 8 & Exhibit 1.

strengthen CPNI privacy protections.⁴⁶ These contract provisions interfere with a CLEC's ability to protect their customer's information in accordance with their own policies and the Commission's rules. The Commission should make clear that the language included in AT&T's commercial agreement and any other language that hampers a carrier's ability to protect the CPNI of its own customers will be deemed unenforceable.

IV. THE COMMISSION SHOULD NOT APPLY ITS CURRENT CPNI RULES OR ANY RULES ADOPTED AS A RESULT OF THIS PROCEEDING TO INTERNET SERVICE PROVIDERS OR INFORMATION SERVICES

The Joint Commenters support the comments in this proceeding arguing that any CPNI requirements should not be applied either to Internet Service Providers ("ISPs") or to non-telecommunications services (such as information services) provided by telecommunications providers.⁴⁷ The Joint Commenters agree that section 222 of the Act, which sets forth the definition of CPNI, explicitly limits CPNI to information derived from telecommunications services, and does not apply to records generated through information services.⁴⁸ Therefore, under the statute, the Commission cannot extend CPNI regulations to non-telecommunications services.

Additionally, records derived from non-telecommunications services (such as ISP services) are not the focus of this proceeding. EPIC has identified a specific industry segment that is under attack: "access to *consumer telephone call records*."⁴⁹ Requiring ISPs (and other entities that offer information services) to be subject to CPNI rules will not offer any meaningful solution to deterring and preventing unlawful access to consumer telephone records. Moreover,

⁴⁶ See *id.* at 9.

⁴⁷ See Comments of the United States Internet Service Provider Association ("US ISPA") at 3-5.

⁴⁸ See *id.* at 3-4; see 47 U.S.C. § 222(f) (defining CPNI as information pertaining to "use of a telecommunications service...").

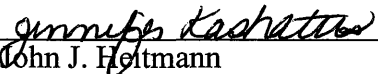
⁴⁹ See Comments of US ISPA at 3.

ISPs and companies that provide non-telecommunications services (including services offered by telecommunications providers) already are responsible for protecting customer information by a number of federal statutes.⁵⁰ Therefore, the Commission should reiterate that, under the plain language of the Act, the section 222 of the Act and the Commission's CPNI rules apply only to telecommunications services provided by telecommunications providers and do not apply to any information services, whether provided by a telecommunications provider or otherwise.

V. CONCLUSION

For the foregoing reasons, the Commission should not modify its existing CPNI rules, but instead should enforce its existing rules and work with the FTC and other state and federal regulatory agencies to curtail unlawful access to and disclosure of CPNI.

Respectfully submitted,


John J. Heitmann
Jennifer M. Kashatus
KELLEY DRYE & WARREN LLP
3050 K Street, NW
Suite 400
Washington, D.C. 20007
(202) 342-8400 (telephone)
(202) 342-8451 (facsimile)

June 2, 2006

⁵⁰ See *id.* at 4-5.

CERTIFICATE OF SERVICE

I, Chris Rathlev, hereby certify that on this 2nd day of June, 2006, I served a true and correct copy of Joint Comments of Echelon Telecom, Inc., SNiP LiNK Inc., and XO Communications, Inc. via U.S. Mail, postage prepaid, unless otherwise noted.

Marlene H. Dortch, Secretary^
Federal Communications Commission
445 12th Street, SW
Washington, D.C. 20554
(Via ECFS)

Janice Myles^
Competition Policy Division
Wireline Competition Bureau
Federal Communications Commission
445 12th Street, SW
Room 5-C140
Washington, D.C. 20554

Best Copy and Printing, Inc. (BCPI)^
Portals II
445 12th Street, SW
Room CY-B402
Washington, D.C. 20554

Chris Jay Hoofnagle
Electronic Privacy Information Center
West Coast Office
944 Market Street, #709
San Francisco, CA 94102

National Association of Attorneys General
of the Undersigned States
750 First Street, NE, Suite 1100
Washington, DC 20002

Princeton University Students
c/o Edward Felten
35 Olden Street
Princeton, NJ 08540

Charter Communications, Inc.
John D. Seiver
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006

Sprint Nextel Corporation
Douglas G. Bonner\
1301 K Street, NW
Suite 600, East Tower
Washington, DC 20005

Qwest Communications
Kathryn Marie Krause
607 14th Street, NW
Suite 950
Washington, DC 20005

T-Mobile USA, Inc.
William F. Maher, Jr.
Morrison & Foerster LLP
2000 Pennsylvania Ave., NW
Washington, DC 20006

T-Mobile USA, Inc.
Thomas J. Sugrue
Kathleen Ham
401 9th Street, NW
Suite 550
Washington, DC 20004

RNK Telecom
Douglas Denny-Brown
333 Elm Street, Suite 310
Edham, MA 02026

Dobson Communications Corporation
Ronald L. Ripley, Esquire
Senior Vice President & General Counsel
14201 Wireless Way
Oklahoma City, OK 73134

BellSouth Corporation
Theodore R. Kingsley
Hubert H. Hogeman III
Suite 4300 West Peachtree Street, N.W.
Atlanta, GA 30375

BellSouth Corporation
Bennett L. Ross
General Counsel – BellSouth D.C.
Suite 900
1133 21st Street, NW
Washington, DC 20036

Attorneys for the California PUC and
the People Of the State of California
Gretchen Dumas
505 Van Ness Avenue
San Francisco, CA 94102

US ISPA
Marc Squillinger
Christian Genetski
Sonnenschein Nath & Rosenthal LLP
1301 K Street, NW
Suite 600, East Tower
Washington, DC 20005

Cingular Wireless
J.R. Carbonell
Carol L. Tacker
M. Robert Sutherland
5565 Glenridge Connector
Suite 1700
Atlanta, GA 30342

Verizon
Karen Zacharia
Joshua E. Swift
1515 N. Court House Road
Suite 500
Arlington, VA 22201

Verizon
Scott Delacourt
Wiley, Rein & Fielding LLP
1776 K Street, NW
Washington, DC 20006

Alltel Corporation
Glenn S. Rabin, Vice President
601 Pennsylvania Avenue, NW
Suite 720
Washington, DC 20004

US LEC
Terry J. Romine
Deputy General Counsel - Regulatory
6801 Morrison Boulevard
Charlotte, NC 28211

NASUCA
Office of the Ohio Consumer's Council
David C. Bergmann
Terry L. Etter
10 West Broad Street, Suite 1800
Columbus, Ohio 43215

National Association of State Utility
Consumer Advocates
Philip F. McClelland
Barrett C. Sheridan
Office of the Consumer Advocate
555 Walnut Street
5th Floor, Forum Place
Harrisburg, PA 17101

NASUCA
Stephen Ward
Paulina McCarter Collins
Main Public Advocate Office
112 State House Station
Augusta, Maine 04333

NASUCA
Robert G. Mork
Indiana Office of Utility Consumer
100 N. Senate Avenue, Room N501
Indianapolis, IN 46204

National Association of State Utility
Consumer Advocates
8380 Colesville Road, Suite 101
Silver Spring, MD 20910

Microsoft/Skype/Yahoo!
A. Richard Metzger, Jr.
Ruth Milkman
A. Renee Callahan
Lawler, Metzger, Milkman & Keeney, LLC
2001 K Street, NW, Suite 802
Washington, DC 20006

NextG Networks, Inc.
T. Scott Thompson
Danielle Frappier
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Ave., NW, Suite 200
Washington, DC 20006

AT&T Inc.
Davida Grant
Gary Phillips
Paul K. Mancini
1401 Eye Street, NW, Suite 1100
Washington, DC 20005

National Cable & Telecommunications
Associate
Daniel Brenner
1724 Massachusetts Avenue, NW
Washington, DC 20036

MetroPCS Communications, Inc.
Wilmer Cutler Pickering Hale and Door
Lynn R. Charytan
1875 Pennsylvania Avenue, NW
Washington, DC 20006

Global Crossing North America, Inc.
Latham & Watkins LLP
Jeffrey A. Marks
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004

Laura H. Parsky
Deputy Assistant Attorney General
United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Elaine M Lammert
Federal Bureau of Investigation
United States Department of Justice
J. Edgar Hoover Building
935 Pennsylvania Avenue, NW
Room 7435
Washington, DC 20535

Independent Carrier Group
Woods & Aitken, LLP
Thomas J. Moorman
2154 Wisconsin Avenue, NW
Suite 00
Washington, DC 20007

Leap Wireless International, Inc.
Latham & Watkins
Jim Barker
555 11th Street
Suite 1000
Washington, DC 20004

Verizon Wireless
John T. Scott, III
Charon H. Phillips
1300 I Street, NW
Suite 400 West
Washington, DC 20005

Time Warner Telecom
Willkie Farr & Gallagher
Thomas Jones
1875 K Street, NW
Washington, DC 20006

Texas Statewide Telephone Cooperative
Cammie Hughes
3721 Executive Center Drive
Suite 200
Austin, Texas 78731

TCA, Inc.
1465 Kelly Johnson Blvd.
Suite 200
Colorado Springs, CO 80920

National Telecommunications Cooperative
Jill Canfield
Daniel Mitchell
4121 Wilson Blvd., 10th Floor
Arlington, VA 22203

United States Telecom Association
Robin E. Tuttle
607 14th Street, NW
Suite 400
Washington, DC 20005

Time Warner Inc.
800 Connecticut Ave., NW
Suite 800
Washington, DC 20006

Electronic Privacy Information Center
Chris Jay Hoofnagle
1718 Connecticut Ave., NW #200
Washington, DC 20009

Electronic Privacy Information Center
Chris Jay Hoofnagle
West Coast Office
944 Market Street, #709
San Francisco, CA 94102

Enterprise Wireless Alliance & USMSS,
Inc.
Elizabeth R. Sachs, Esq.
Lukas, Nace, Guitierrez & Sachs
1650 Tysons Boulevard
Suite 1500
McLean, VA 22102

COMPTEL
Jason Oxman
Mary C. Albert
1900 M Street, NW
Suite 800
Washington, DC 20036

Pennsylvania Public Utility Commission
Joseph K. Witmer
P.O. Box 3265
Harrisburg, PA 17105

NJ Division of the Ratepayer Advocate
Seema M. Singh
Christopher J. White
31 Clinton Street, 11th Floor
P.O. Box 46005
Newark, NJ 07101

Centennial Communications Corp.
Danielle Frappier
Cole, Raywid & Braverman, LLP
1919 Pennsylvania Ave., NW
Suite 200
Washington, DC 20006

American Association of Paging Carriers
Kenneth E. Hardman
2154 Wisconsin Avenue, NW
Suite 250
Washington, DC 20007

OPASTCO
Brian Ford
Stuard Polikoff
21 Dupont Circle, NW
Suite 700
Washington, DC 20036

USA Mobility, Inc.
Latham & Watkins LLC
Mattheew Brill
555 11th Street, NW
Suite 1000
Washington, DC 20004

CTIA – The Wireless Association
Michael F. Altschul
Christopher Guttman-McCabe
1400 16th Street, NW
Suite 600
Washington, DC 20036

A handwritten signature in black ink, appearing to read "CHRATHLEV", written over a horizontal line.

Chris Rathlev

^ Via email